# Michael A. Lodder

redmike7@gmail.com
(801) 573-0773
github: mikelodder7

# PROFESSIONAL EXPERIENCE

**Freelance Developer and operations engineer,** Lodder Software Engineering LLC, 2016-Present
I do contract work for companies and individuals for various tasks with software and cloud development. I also perform security audits, reverse engineering, and malware analysis.

- Cloud development in AWS, Azure, Rackspace, and GCP with Terraform
- I work regularly with Hashicorp Vault, Nginx, Apache Web Server, MySQL, SQL Server, Redis, SQLite, SQLCipher
- Written projects in C#, Java, Scala, Rust, C++, C, Perl, Python, PHP, Golang, NodeJS
- I advise companies how to improve their system security architecture, protocols, and crypto suites.
- Published many of Rust crates and contributed to lots of others. Most in the realm of cryptography, Zero-knowledge Proofs and reverse engineering
- Member of RustCrypto group responsible for publishing and maintaining cryptography libraries in Rust.
- Published many Golang cryptography based modules

---

**Cryptography Engineer,** *HorizenLabs,* Nov 2022-Present
Design, architect, and write code for complex cryptographic algorithms and services related to Web3 products.

- Cryptographic Code in Java and Rust
- Designed Cryptography as a service API

**Staff Applied Cryptographer,** *Coinbase Inc.*, May 2020-Dec 2022
Design, architect, and lead teams of cryptographers and security engineers. My focus is on secure multiparty computation for threshold signing and encryption for protecting digital assets. Latest development is on decentralized identity for DeFi and blockchain exchange of PII.

- Coinbase has many needs for certified anonymous access to its data and APIs to be compliant with CCPA, GDPR, and PCI.
- These privacy enhancing techniques focus on data minimization, selective disclosure, and information hiding.
- Other work includes leading integration efforts for Web3, adding digital assets, and open sourcing cryptography code.
- All programming is with Golang.
- Designed internal introduction to privacy and cryptography course for new engineers
- Mentoring Junior Developers with cryptography
- In charge of open source efforts around Kryptology (https://github.com/coinbase/kryptology)

**Senior Architect Cryptographer**, *Ockam Networks,* June 2020-March 2021
Developed privacy enhancing communication, authentication and authorization protocols for IoT based devices. These protocols include zero-knowledge proof based information sharing for authentication, authorization, and discovery.

**Security Maven**, *Sovrin Foundation,* Provo UT, Sept 2018 - March 2020
I wrote protocols, security policies, implementing crypto, assess networks, and led best practice

security training and code reviews. I performed many responsibilities of CISOs, security and devopsec engineers. I loved coaching and teaching best security practices and programming.

- Codeveloped decentralized key management DKMS practices and a protocol for DHS. Available at https://github.com/hyperledger/indy-sdk/blob/master/docs/design/005-dkms/DKMS%20Design%20and%20Architecture%20V3.md
- Develop many standards and RFCs for key management and programming around HSM/TEE/TPM/Enclave standards
- Participate in the W3C groups for standardizing decentralized identifiers (DIDs) and verifiable credentials. Available at https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html
- Advocate privacy and self sovereign identity and regularly give webinars and visit onsite for instruction.
- Advocate for security and privacy and I enjoy teaching and encouraging best practices. Lately my work and research has been focusing on security and privacy with Blockchains.
- Coordinate weekly with cryptographers in academia and industry to develop new and enhance existing cryptography and open source protocols.
- Security and Software Architect for many of Sovrin's core projects.
- Core maintainer on the hyperledger ursa project, which aims to be all the crypto code for all of hyperledger written primarily in Rust and C.
- Written secure enclave code for Yubico, Apple, Intel SGX, Arm Trustzone
- Core maintainer on hyperledger indy crypto and sdk
- Contribute to many Rust crates
- Write documentation, knowledge base articles, and white papers
    - https://github.com/hyperledger/ursa/blob/master/libindy-crypto/docs/AnonCred.pdf
    - https://forum.sovrin.org
    - https://github.com/hyperledger/indy-hipe/tree/master/text/0024-a2a-forward-secrecy
    - https://github.com/WebOfTrustInfo/rwot7-toronto/blob/master/final-documents/offline-use-cases.pdf
- Maintain security and infrastructure of Sovrin servers and network using terraform and saltstack

---

**Senior Crypto Engineer**, *Evernym Inc.,* Draper, UT June 2017 - Sept 2018

- Researched and developed a decentralized key management systems for Department of Homeland Security and for Sovrin
- Research into applications for efficient forward secret 0-RTT key exchange
- Research for secure hardware and embedded systems like Intel SGX, FPGAs, TPM, securing BYOD.
- Research and development improvements for privacy preserving anonymous credentials and value exchange
- Help create security training material for fellow employees
- Review and test security code written by employees and contractors
- Contribute to indy-sdk for Hyperledger Indy involving cryptography and security programming
- Created an encrypted wallet in Rust for indy-sdk for Hyperledger Indy
- Developing Zero-Knowledge Language in cooperation with IBM-Zurich for describing zero-knowledge proofs so software engineers can understand the cryptography math and know how to implement in code

---

**Senior Security Engineer**, *Sawtooth Software Inc.,* Orem, UT May 2008 - June 2017
Software development group.

- Have a passion for cryptography and all things security
- Looking for ways to apply Ethereum to data collection for secure data collection in ad hoc manner across mobile devices and secure identity management
- Responsible for all company security policies in software development life cycle using the STRIDE and DREAD model and the OWASP Top 10 vulnerabilities. Used Rapid7

AppSpider, nmap, Nessus, Burp Suite, DirBuster, Skipfish, Wapiti, SQLmap, John the Ripper, Metasploit, Nexpose, Wireshark, Charles, and Qualys tools like SSLLabs
- Developed cryptographic security guidelines and process with APIs
- Review client contracts to ensure internal security compliance and customer clarification
- Help customers meet HIPAA/PCI DSS requirements using our software for data collection transmission and handling
- Helped develop disaster recovery plan and business continuity plan
- Developed security awareness training
- In charge security technical training like teaching Symmetric and Asymmetric algorithms
- In charge of risk assessment meetings and security assessment both internal and from 3rd parties
- Presented company security training and awareness training meetings
- Written company data classification policy and data handling policy
- Developed company security policies and standards for handling and encrypting customer and internal sensitive data and key rotation.
- Developed secure methods for programmers to access cloud infrastructure while tracking access and auditing with SSH, ScaleFT, VPN, and Bastion Hosts running Ubuntu
- Developed company's first mobile app for Android in Java, Typescript, nodejs, the server backend with JSON Swagger API's and Perl. Further developed a C# app for Ubuntu for downloading with pause/resume methods for Perl on Android. Figured out how to get Perl running natively on Android devices
- Upgraded company web stack from Apache suEXEC, MySQL single server to Nginx, custom programmed FastCGI with suEXEC like behavior in C, and Cloud MySQL loadbalanced system running GlusterFS for Rackspace Cloud
- Spearheading migration from Rackspace Cloud to Amazon AWS
- Spearheading development for MySQL to Apache Cassandra migration
- Use SaltStack, Hubblestack, and Python for infrastructure, security and deployment automation in Rackspace Cloud and Amazon AWS with Ubuntu Linux. Hubblestack for OS Sec, auditing, reporting, and compliance, Fail2ban for IPS, and Nginx+ with Modsecurity for WAF.
- Used terraform to build Azure, AWS, and Rackspace cloud infrastructure for autoscaling
- Helped migrate all company source control from Visual Source Safe and Subversion to Mercurial and now to Git and TFVC.
- Developed company's first cloud product in Rackspace Cloud in PHP, Javascript, Bash, and Perl.
- Wrote internal web application automation and load testing tool in Scala, again in Go, and again in C#.
- Wrote internal XLIFF editor in Scala
- Helped rewrite VB6 code to C# in WinForms and WPF.
- Programmed flagship desktop application in VB6, Perl, and C++.
- Programmed Java Web Application for Tomcat and Ubuntu on the web and Swing for the desktop.
- Annually prepare the devops and infrastructure budget, monitor it throughout the year.
- Taught classes and presented at my company's 18 month cycle conference.

**Graduate Research Assistant,** *University of Utah,* Salt Lake City, UT 2007-2009
School of Computing
- Research in mobile computing in low power and reducing time overhead using predictive measurements in low power circuits related to biological networks.
- Programmed many automation tools in Perl and Python for CentOS and Redhat Linux, and Sun Solaris.
- Researched speech algorithms for low power on Coldfire and ARM microchips.

Advisor: Prof. Al Davis

**Co-op Engineer,** *L-3 Communications CSW,* Salt Lake City, UT 2006-2008

Hardware/Software Engineering Group.

- Developed software and hardware for data links and projects used for intelligence gathering and reconnaissance.
- Programmed in C/C++ and Assembly for Unix, BSD , Solaris, GreenHills Integrity, and VxWorks using make files and gcc, Visual Studio, and Intel compilers.
- Programmed VHDL for Xilinx and Altera FPGAs and CPLDs.
- Implemented TPMs in VHDL for safeguarding system hardware and software.
- Involved in software testing and automation, ensuring security compliance with appropriate engineers using Nessus vulnerability scanner, Burp Suite, nmap, and inhouse tools for DCID 6/3 and DIACAP. Involved with final signing off of multiple government projects.
- Most of the scripts and automation were developed in Bash, Perl, Tcl, and VB6.
- Programmed security protocols like TwoFish and AES in C/C++ since OpenSSL was declared unsafe and used developed in house tools for testing that I wrote in C# with WinForms, others in Java with GWT in Eclipse and IntelliJ.
- Programmed in house networking protocols to shorten the OSI stack and tested them with self written programs in C# and Java.
- Worked with multiple teams across the company, Boeing, BAE Systems, and Lockheed Martin to ensure all requirements had been met, code was securely shared and delivered.
- Developed multiple internal applications to help with internal project development and status tracking in C#, ASP.NET, Javascript, and SQL Server using Visual Studio.
- Developed many plugins/hooks for Rational Rose ClearCase in Perl, Bash, and Tcl. Automated project build processes with Perl, Bash, and Tcl.
- The company grew from 2000 employees to over 3000 employees while I was there. My division doubled in the 2 years I was there, which made it fast paced for development. Many projects were developed quickly to be deployed to JSOC and Air Force in less than 72 hours.
- Implemented software in Perl and Java for preparing and configuring military grade laptops and ensured FIPS compliance.

# EDUCATION

**Ph.D, Cyber Operations** Anticipated 2022
Dakota State University – Madison, SD

**M.S., Electrical Engineering** 2008
Thesis – Biologically Motivated Predictions for Dynamic Power in VLSI Circuits
Advisor – Prof. Al Davis
University of Utah – Salt Lake City, UT

**B.S., Computer Engineering** 2008
University of Utah – Salt Lake City, UT

# LANGUAGES

- English
- Spanish

# PROFESSIONAL REFERENCES

Ken Ebert, *Indicio.Tech,* Provo UT
Chief Technical Officer

Email - ken@indicio.tech

Nathan George, *Kiva,* Lehi UT
Senior Director of Engineering, Protocol
Phone - 801-360-9647

Adam Everspaugh, *Coinbase*
Phone - 321-626-2400
Email - adam@everspaugh.com

Phil Windley, *Brigham Young University,* Provo UT
Phone - 801-362-5611
Email - phil@windley.org

Aaron Hill, *Sawtooth Software Inc.*, Orem, UT
Vice President Client Services
Phone - (801) 477-4700 x120
Email - aaron@sawtoothsoftware.com